**Конкурсное задание**

Компетенция

(Сетевое и системное

администрирование 14-16)

# Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Задание
4. Критерии оценки

Количество часов на выполнение задания: 12ч.

* 1. **ФОРМЫ УЧАСТИЯ В КОНКУРСЕ**

Командный конкурс, команда 2 человека.

* 1. **ЗАДАНИЕ ДЛЯ КОНКУРСА**

Содержанием конкурсного задания является Создание и настройка сетевой инфраструктуры дома или небольшого офиса. Участники соревнований получают инструкцию и топологию сети. Конкурсное задание сквозное и выполняется в течении 3х дней.

Конкурс включает в себя выполнение пуско-наладочных работ сетевого и пользовательского оборудования.

Окончательные аспекты критериев оценки уточняются оценивающими экспертами. Оценка производится ежедневно по окончании работ. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены оценивающими экспертами.

***Предисловие***

Используемые версии ПО

| **Машины** | **ОС** |
| --- | --- |
| BR, GW | OPNSense |
| HQRTR | Linux (VyOS) |
| LINCLI, REMOTECLI,BRCLI | Debian 10 (MATE), English |
| LINSRV, WEBSRV,BRSRV,LINRTR | Debian 10 (CLI) |
| WINSRV | Windows Server 2019 Standard(GUI) |
| WINCLI | Windows 10 Education, English |
| WDSCLI | Отсутствует |

Исходная настройка

При выполнении задания учитывайте информацию из этого раздела.

В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль **P@ssw0rd**.

На маршрутизаторе HQRTR логин/пароль по умолчанию - **vyos**/**vyos**

На межсетевых экранах BR и GW логин/пароль по умолчанию - **root**/**opnsense**

При выполнении настоящего задания всегда нужно руководствоваться **правилом наименьших привилегий**.

На сетевых устройствах сделаны базовые сетевые настройки:

* На маршрутизаторе HQRTR на подынтерфейсе eth1.1 и интерфейсе eth0 настроены IPv4-адреса для сети FLOOR1 и для соединения с межсетевым экраном GW, а также статический маршрут по

умолчанию в сторону GW.

* На межсетевом экране GW настроен IPv4-адрес на внутреннем интерфейсе, добавлен статический маршрут до сети FLOOR1 через HQRTR, DHCP выключен, остальные настройки по умолчанию.
* На BR все настройки по умолчанию.

### Управление HQRTR осуществляется через локальную консоль.

Управление GW осуществляется через Web-интерфейс с устройств в сети FLOOR1. Управление BR осуществляется через Web-интерфейс с устройств в сети BRANCH. На BR и GW дополнительно доступна локальная консоль.

На машине WEBSRV установлены и работают следующие службы:

* FTP

– Адрес: 3.14.15.126

* + Логин ftpuser
  + Пароль ftppass
* Веб-сервер обслуживает сайты:
  + jun.ru
  + worldskills.ru
* DNS

### Консольный доступ к виртуальной машине WEBSRV для участника не предполагается.

На всех Linux машинах существует пользователь **root** с паролем **toor** и пользователь **skill39** с паролем **P@ssw0rd**

### В дисководе оптических дисков машины WINSRV установлен диск с дистрибутивом Windows 10 Education.

***Задание***

### Схема IP-адресации.

| Сеть | Устройство | Адрес/Маска | Интерфейс |
| --- | --- | --- | --- |
| Internet | GW | 3.14.15.92/25 | em1 |
|  | BR | 3.14.15.15/25 | em1 |
|  | LINRTR | 3.14.15.75/25 | ens192 |
|  | Шлюз провайдера | 3.14.15.126 |  |
|  | DNS-серверы | 3.3.4.4  3.14.14.3 |  |
| Floor1 | HQRTR | 192.168.1.1/24 | eth1.1 |
|  | LINCLI | DHCP |  |
|  | WINCLI | DHCP |  |
|  | WINSRV | 192.168.1.10/24 |  |
| Floor2 | HQRTR | 192.168.2.30/27 | eth1.2 |
|  | WDSCLI | DHCP |  |
|  | LINSRV | 192.168.2.8/27 |  |
| GW-HQRTR | GW | 192.168.0.1/30 | em0 |
|  | HQRTR | 192.168.0.2/30 | eth0 |
| Branch | BR | 192.168.10.1/28 | em0 |
|  | BRCLI | DHCP |  |
|  | BRSRV | 192.168.10.10/28 |  |
| LINRTR LAN | LINRTR | 192.168.20.1/29 | ens224 |
|  | REMOTECLI | DHCP | ens192 |

День 1

*Настройка сети*

1. Настройте имена устройств согласно топологии.

| HQRTR vyos/vyos  configure режим конфигурации  set system host-name HQRTR имя  commit приметь (discard -отменить) |
| --- |

1. Настройте доменное имя JunWin.wsr на GW и HQRTR.

| HQRTR  set system domain-name JunWin.wsr доменное имя  commit |
| --- |

1. Настройте учётные записи на сетевых устройствах GW, BR и HQRTR.
   1. Используйте логин js и пароль JSfinals2020
   2. Пользователь с логином js должен иметь максимальные полномочия на сетевых устройствах.

| HQRTR  edit system login user js  set authentication plaintext-password JSfinals2020  set level admin  commit  save  save |
| --- |

1. Настройте IPv4-адреса и шлюз по умолчанию на внешних интерфейсах GW, BR, LINRTR согласно схеме адресации.
2. Настройте IPv4-адреса на устройствах в сети первого этажа (FLOOR1).
3. Настройте IPv4-адреса для сети второго этажа (FLOOR2) согласно следующим требованиям:
   1. Используйте на HQRTR подынтерфейс с номером VLAN 2.
   2. Настройте описание подынтерфейса 'FLOOR2'.
   3. Используйте маску подсети /27.

| HQRTR | |
| --- | --- |
| show interfaces | Смотрим текущую конфигруацию |
| edit interfaces ethernet eth1 |  |
| set vif 2 address 192.168.2.30/27 |  |
| set vif 2 description FLOOR2 |  |
| commit |  |
| save |  |
| show interfaces |  |

1. Настройте DHCP Relay на маршрутизаторе HQRTR таким образом, чтобы клиентам в сети FLOOR2 адреса выдавал сервер WINSRV.

| set service dhcp-relay interface eth1.1  set service dhcp-relay interface eth1.2  set service dhcp-relay server 192.168.1.10  commit  save |
| --- |

1. Обеспечьте выход в интернет для всех устройств центрального офиса.
   1. Настройте дополнительную маршрутизацию там, где это требуется.
   2. Настройте межсетевой экран и NAT на GW.
   3. Сделайте другие необходимые настройки, чтобы устройства центрального офиса могли выйти в интернет и зайти на сайты jun.ru и worldskills.ru
2. Настройте сетевое обнаружение по протоколам CDP и LLDP на всех сетевых устройствах (GW, HQRTR, LINRTR, BR) и на серверах LINSRV и BRSRV.

| HQRTR:  set service lldp  commit  save |
| --- |

1. Настройте корректное время и часовой пояс Europe/Moscow на сетевых устройствах.

| HQRTR:  set system time-zone Europe/Moscow  commit  save |
| --- |

1. Настройте NTP.
   1. В качестве сервера должен выступать HQRTR
      1. Настройте в качестве клиентов LINCLI и WINSRV

| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Зайти с LINCLI на GW: root/opnsense \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Имя, часовой пояс\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Используйте логин js и пароль JSfinals2020\_\_\_\_\_\_\_\_\_\_\_\_\_\_      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Настройка WAN\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Firewall на BR и GW\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_              \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Nat на BR и GW\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_            \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Зайти с BRCLI на BR: root/opnsense\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Используйте логин js и пароль JSfinals2020\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Настройка WAN\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_        \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Настройка DNS на BR и GW\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_    \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ BR GW: протоколы CDP и LLDP \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- |

*Настройка Linux*

1. Настройте имена устройств согласно топологии.

| Надо сделать на LINCLI, REMOTECLI,BRCLI, LINSRV, WEBSRV,BRSRV,LINRTR  echo ИМЯ > /etc/hostname  или через  apt install network-manager (установка nmtui)  nmtui – set system hostname -- ИМЯ |
| --- |

1. Настройте IP адреса на серверах LINSRV, BRSRV согласно схеме адресации.

| LINSRV  nmtui – edit a connect – wired connect |
| --- |

1. Настройте общий доступ к файлам на LINSRV по протоколу NFS.
   1. Каталог для хранения файлов **/opt/nfs/rw** должен быть доступен для чтения и записи.
   2. Каталог для хранения файлов **/opt/nfs/ro** должен быть доступен только для чтения.
   3. NFS должен быть доступен для клиентов в сети FLOOR1.

| apt install nfs-kernel-server -y |  |
| --- | --- |
| mkdir /opt/nfs/rw -p  mkdir /opt/nfs/ro -p | создаем каталоги с ключом “p” (подкаталоги) |
| nano /etc/exports | Редакт конфиг файл |
| Дописываем внизу  /opt/nfs/ro 192.168.1.0/24(ro,sync,no\_subtree\_check,all\_squash,anonuid=1001)  /opt/nfs/rw 192.168.1.0/24(rw,sync,no\_subtree\_check,all\_squash,anonuid=1001) | |
| reboot | |

* 1. Настройте клиент NFS на LINCLI.
     1. В качестве сервера используйте LINSRV.
     2. Путь **/opt/nfs/rw** на LINSRV должен быть смонтирован в каталог

**/home/skill39/Desktop/nfs\_rw** на LINCLI.

* + 1. Путь **/opt/nfs/ro** на LINSRV должен быть смонтирован в каталог

**/home/skill39/Desktop/nfs\_ro** на LINCLI.

* 1. Каталог **/home/skill39/Desktop/nfs\_rw** на LINCLI должен быть доступен для чтения и записи для пользователя **skill39**.
     1. Каталог **/home/skill39/Desktop/nfs\_ro** на LINCLI должен быть доступен только для чтения для пользователя **skill39**.
     2. Монтирование должно восстанавливаться при перезагрузке виртуальной машины.

| Зайти под skill39/P@ssw0rd, открываем терминал |  |
| --- | --- |
| pwd | Посмотреть текущий каталог |
| mkdir /home/skill39/Desktop/nfs\_rw  mkdir /home/skill39/Desktop/nfs\_ro | Создаем папки по заданию |
| su | toor |
| apt install nfs-common -y |  |
| nano /etc/fstab | Редактируем файл |
| 192.168.2.8:/opt/nfs/rw /home/skill39/Desktop/nfs\_rw nfs  192.168.2.8:/opt/nfs/ro /home/skill39/Desktop/nfs\_ro nfs | В конец файла. Монтируем папки ro и rw на клиенте |
| sudo reboot |  |
|  |  |

* 1. Настройте централизованный сбор журналов syslog на LINSRV.
     1. Журналы должны храниться в файле **/opt/logs/errors.log**
     2. LINCLI должен записывать сообщения **error и более важные**.
     3. GW должен записывать системные сообщения (**System Events**).
  2. Установите пакет **sudo** на LINSRV.

| apt install sudo -y |
| --- |

* 1. Создайте пользователя **admin** с паролем **P@ssw0rd** на LINSRV.
     1. Добавьте пользователя **admin** в группу **sudo**.

| adduser admin    P@ssw0rd  P@ssw0rd  5 enter  y enter  adduser admin sudo |
| --- |

* 1. Настройте права доступа для каталога **/opt/nfs/**.
     1. Пользователь **admin** должен иметь права на чтение и запись в каталог **/opt/nfs** и все его подкаталоги.

| chown admin /opt/nfs –R  ls –l /opt/nfs |
| --- |

* 1. Настройте LINRTR для обеспечения доступа в интернет для клиентов локальной сети.
     1. Настройте DHCP для локальной сети.
     2. Используете адрес LINRTR в качестве адреса DNS сервера для клиентов сети.
     3. Настройте NAT для адресов в локальной сети.

| apt install network-manager isc-dhcp-server iptables-persistent –y | |
| --- | --- |
| внешний интерфейс | внутренний |
| nano /etc/default/isc-dhcp-server (указываем внутренний интерфейс)  https://sun9-47.userapi.com/impg/7DVUGGjwnUfmOyoceEJynW-Zan9JXoH63p3miQ/mG7YDIGfD0k.jpg?size=789x264&quality=96&proxy=1&sign=ed33ce2e6c2c524bf1b65a8f6bc38fda&type=album | |
| nano /etc/dhcp/dhcp/dhcpd.conf  https://sun9-42.userapi.com/impg/1EScPXWz985mbf1QxI07_APiNCJQoD14Uk-zWw/K98CJwf-j28.jpg?size=727x524&quality=96&proxy=1&sign=6e34062c116f13741196d1dec0e9e41c&type=album | |
| iptables -t nat -A POSTROUTING -o ens224 -j MASQUERADE iptables-save > /etc/iptables/rules.v4 | |

## Настройка Windows

1. Настройте имена устройств на первом этаже согласно топологии.
2. WINSRV, WINCLI и WDSCLI должны отвечать на запросы по протоколу ICMP.

#### Настройка WINSRV

1. Настройте сетевой интерфейс на WINSRV согласно схеме адресации.
2. Установите основной контроллер домена JunWin.wsr и основной DNS-сервер, полномочный для зоны JunWin.wsr.
3. Создайте доменные группы Engineers и Workers.
4. В группе Workers создайте пользователей Denis и AlexS. В группе Engineers создайте пользователей NikS и AlexT. Все пользователи в домене должны менять пароль на новый не позже, чем через 10

дней.

1. Разрешите членам группы Engineers локальный вход на контроллер домена.
2. Настройте DNS-зоны прямого и обратного просмотра, необходимые для клиентских компьютеров, расположенных на первом и втором этажах.
3. Настройте пересылку неизвестных DNS-запросов на серверы 3.3.4.4 и 3.14.14.3.
4. Настройте DHCP-сервер, способный выдавать адреса всем клиентским компьютерам, находящимся на первом и втором этажах.
5. Настройте WDS-сервер. Используйте дистрибутив ОС, находящийся в дисководе оптических дисков. Для хранения установочных файлов используйте дополнительный жесткий диск, системный жесткий диск для этих целей использовать запрещается! Право устанавливать ОС по сети должны иметь члены группы доменных администраторов и члены группы Workers. Обеспечьте согласованную работу сервиса со службой DHCP. После установки ОС компьютеры должны автоматически входить в домен с именами WDSCLI1, WDSCLI2 и т.д.
6. Для всех клиентских компьютеров домена должна быть отключена приветственная анимация.

| НАСТРОЙКА WINSRV  Открываем PowerShell или cmd и пишем slmgr /rearm после нажимаем ОК.  Сброс лицензии windows server – что бы не выключаться каждый час.    Настройка адреса    Настрой имени    Установка ролей    Галочка>Yes>Install    Делаем домен JunWin.wsr > Нажимаем на флажок > Promote this server to a domain controller    Создаём новый домен > JunWin.wsr > Next    Пароль: P@ssw0rd > Next > Next > Next > Next > Next > Install    DHCP > Complete DHCP configuration > Next > commit > Close    Tools > DNS      Next > Next > Next > Next >    Next > finish  Так же для 2 этажа    Tools > DHCP > New Scope > start add (192.168.1.1) end add (192.168.1.254) length (24)    Исключаем два адреса    Добавляем шлюз > next > next > ok    Так же создаем пул для 2 этажа        Создание групп > Tools > Active Directory Users and Computers > По JunWin.wsr правой кнопкой > organization unit > Убираем галочку и пишем имя    Правой кнопкой по Engineers > New > Group > Пишем Engineers > OK    Создаём пользователей в и загоняем в группу Workers  Workers правой кнопкой > New > Add User > Denis > пароль: P@ssw0rd  Workers правой кнопкой > New > Add User > AlexS > пароль: P@ssw0rd    Так же и в Engineers только другие пользователи и группы      Разрешаем ICMP  Tools > Group Policy management > Правый клик по Default domain > Edit    Политика находится по пути - Computer Configuration → Policies → Windows Settings → Security Settings → Windows Defender… → Windows Defender… → Inbound Rules      Next > Next > Next > Next > Next > Next >любое имя> finish  Создаём политику что бы пользователи меняли пароль через 10 дней  Windows Settings > Security Setting > Password Policy > Maximum password age > (10) > ok > открываем powershell: пишем gpupdate /force    Создание политики для отключения анимации  Tools > Group Policy Management > Правый клик по Default domain > Create GPO > name (NoAnim) > Edit > Computer Configuration > Polices > Administrative Template > System > Logon > Show first sing-in animation > Disable > Apply > Ok > открываем powershell: пишем gpupdate /force |
| --- |

#### Настройка WINCLI

1. Сделайте компьютер членом домена JunWin.wsr.
2. На компьютере должна быть только одна локальная учетная запись пользователя - Administrator.

| НАСТРОЙКА WINCLI  Заходим под пользователем которого создали, включаем учетку администратора  Right Click windows icon > Computer Manager > Users > Administrator > disabled (убрать галочку)    Right Click windows icon > Computer Manager > Users > Удаляем всех пользков кроме администратора    Right Click windows icon > System > System info > Change Settings > Computer name: WINCLI    Right Click windows icon > System > System info > Change Settings > Domain: JunWin.wsr >  Username: Administrator  Password: (P@ssw0rd) > reboot    Other User > User Name : (JunWin\Administrator) > Password: (P@ssw0rd) |
| --- |

#### Настройка WDSCLI

1. Установите на компьютер ОС Microsoft Windows 10 Education.
2. Обеспечьте членство компьютера в домене JunWin.wsr.
3. На компьютере должна быть только одна локальная учетная запись пользователя - Administrator.

День 2

## Настройка сети

1. Настройте сеть филиала BRANCH
   1. На межсетевом экране BR поменяйте адрес внутренней сети, чтобы он соответствовал схеме IP-адресации.

| Заходим с BRCLI меняем адрес |
| --- |
| Назначаем адрес BRCLI 192.168.10.2/28 |

* 1. Настройте DHCP-сервер на BR, чтобы он выдавал следующие настройки:
     1. Сеть и маска согласно схеме адресации
     2. Шлюз - BR
     3. Адреса DNS-серверов - 3.3.4.4 и 3.14.14.3
     4. Домен - branch
     5. Диапазон адресов - с .3 по .8 включительно.

| Получаем адрес по dhcp |
| --- |

* 1. Настройте NAT и межсетевой экран таким образом, чтобы был обеспечен выход в интернет для всех устройств филиала.
  2. Настройте IPsec между GW и BR для связи филиала и домашнего офиса со следующими параметрами:
     1. Протокол IKEv2.
     2. Параметры согласования IKEv2 - AES128, SHA256, DH15, аутентификация по общему ключу.
     3. Параметры IPsec - Режим Tunnel, защита ESP AES128, SHA256
     4. Туннель должен обеспечивать связь через защищённый канал между филиалом BRANCH и сетью FLOOR1 центрального офиса.

| 1 фаза:        На BR то же самое, только меняется адрес шлюза    Разрешаем ipsec на BR и GW    Листаем до конца и сохраняем на BR и GW!!    2 фаза:  На BR              На GW              Запустить: |
| --- |

1. Настройте OSPFv2 между HQRTR и GW
   1. Используйте область 0.
   2. GW должен узнавать о сетях FLOOR1 и FLOOR2 через OSPF. Не используйте на GW статические маршруты до этих сетей.

|  |
| --- |

* 1. HQRTR должен получать маршрут по умолчанию и другие необходимые маршруты от GW через OSPF. Не используйте статические маршруты на HQRTR.
  2. Интерфейсы в сторону сетей FLOOR1 и FLOOR2 на HQRTR должны быть настроены как пассивные.

| set protocols ospf area 0.0.0.0 network 192.168.1.0/24  set protocols ospf area 0.0.0.0 network 192.168.2.0/27  set protocols ospf area 0.0.0.0 network 192.168.0.0/30  set protocols ospf passive-interface eth1.1  set protocols ospf passive-interface eth1.2  set protocols ospf neighbor 192.168.0.1  commit  save |
| --- |

## Настройка Linux

1. Настройте службу DNS на LINRTR.
   1. LINRTR должен выполнять трансляцию DNS запросов (DNS Proxy) от локальных клиентов.
   2. Используйте для проверки адрес jun.ru.

| apt install bind9 | устанавливаем DNS сервер |
| --- | --- |
| nano /etc/bind/named.conf.options | редактируем конфигурационный файл |
| options {  forwarders { 3.3.4.4;  3.14.14.3; } ;  forward first;  listen-on { any;};  recursion yes;  allow-query { any; };  dnssec-validation no;  listen-on-v6 { none; };  } | Включаем перенаправление неизвестных DNS запросов  Какие адреса принимают DNS запросы  Включаем рекурсивные запросы  Разрешаем всем выполнять запросы  Отключаем dnssec  Отключаем DNS запросы по ipv6 |
| systemctl restart bind9 | Перезапустить DNS сервер |
| systemctl status bind9 | Посмотреть статус работы DNS сервера |

1. На BRSRV настройте веб-сервер.
   1. Файлы веб-сайта должны располагаться в каталоге **/var/www/**
   2. Сайт должен быть доступен по локальному IP адресу для клиентов сети BRANCH.
   3. Сайт должен быть доступен по IP адресу BR для клиентов сети Internet.

| apt install network-manager apache2 –y | устанавливаем network-manager, apache2 |
| --- | --- |
|  | |

* 1. Веб-сайт должен работать по протоколу HTTPS.
     1. Настройте автоматическую переадресацию протокола HTTP на HTTPS.
     2. Используйте самоподписанные сертификаты. Доверие сертификатам со стороны клиентов не требуется.

## Настройка Windows

#### Настройка WINSRV

1. Установите и настройте доменный корневой центр сертификации с именем ROOTCA и сроком действия основного сертификата 6 лет.
2. Установите и настройте web-сервер.
3. Установите и настройте ftp-сервер.
4. Создайте сайт, доступный клиентам, находящимся на первом и втором этаже, по имени home.junwin.wsr. Тело сайта, файл c:\Site\index.htm:

#### <html>

**<body>**

**<center>**Hello, World!!!**</center>**

#### </body>

**</html>**

Сайт должен быть доступен только по протоколу HTTPS. Сертификат безопасности должен быть выдан ROOTCA. При обращении к сайту по протоколу HTTP должно включаться автоматическое перенаправление на протокол HTTPS.

1. На контроллере домена в браузере IE в качестве домашней страницы должно использоваться

содержимое папки, содержащей актуальный список отзыва сертификатов для ROOTCA. Список отзыва сертификатов должен быть доступен для скачивания по нажатию на ссылку.

1. На клиентах домена в браузере IE в качестве домашней страницы должен использоваться сайт [home.junwin.wsr](http://home.junwin.wsr).

| Настройка WINSRV  Установка сертификации с именем ROOTCA и сроком 6 лет  Screenshot_3  Screenshot_4  Screenshot_5  Screenshot_6  После установки  Screenshot_7  Screenshot_8  Screenshot_9  Screenshot_10  Screenshot_11  Screenshot_12  Screenshot_13  Screenshot_14  Screenshot_15  Screenshot_17  Screenshot_18  Создание тело сайта  Переходим на диск C>создаём папку Site>в папке Siteсоздаём текстовый файл с названием index> (Полный путь ***c:\Site\index***)  Screenshot_19  Пишем данные из задания и сохраняем  Screenshot_20  ВпроводникенажимаемнавкладкуView>Filenameextensions> rename index.txt > index.html  Screenshot_21  Создаём политику или редактируем стандартную    Screenshot_22  C:\Users\User\Desktop\Документы\Скрины\Screenshot_23.png  После того как написали https://[home.junwin.wsr](http://home.junwin.wsr) надо нажать F5    Потом тоже самое в другом подразделении    Там же  **Computer Configuration - Policies -> Administrative Templates -> System -> Group Policy** . У нее два режима работы — **Replace (Замена) и Merge (Слияние)**.    Настройка WEB-server  C:\Users\User\Desktop\Документы\Скрины\Screenshot_25.png  Screenshot_26  Screenshot_27  Screenshot_28  Здесь ставим галочку    А здесь снимаем    И здесь снимаем    Включаем просмотр каталога |
| --- |

День 3

## Настройка сети

1. Настройте проброс портов на BR. Веб-сервер на BRSRV должен быть доступен из интернета по адресу внешнего интерфейса BR и портам 80 и 443.
2. Настройте OpenVPN
   1. OpenVPN-сервером должен быть GW.
   2. Используйте хеширование SHA-256 и шифрование AES.
   3. Клиентом будет REMOTECLI
   4. Используйте аутентификацию по логину **jsremote** и паролю **JSopenvpn**
   5. У клиента должна быть связь с сетью FLOOR1
   6. Используйте WINSRV в качестве DNS-сервера

## Настройка Linux

1. По протоколу FTP получите файлы сайта на сервере провайдера WEBSRV и поместите полученное в каталог **/var/www/**
2. Настройте удаленный доступ по протоколу SSH для LINRTR.
   1. SSH сервер должен принимать подключения только из локальной сети.
   2. REMOTECLI должен выступать клиентом удаленного доступа по протоколу SSH.
   3. Доступ к LINRTR для пользователя **skill39** должен происходить с помощью аутентификации на основе открытых ключей (без ввода логина и пароля).

| LINRTR  apt install openssh-server  vim /etc/ssh/sshd\_config  ListenAddress 192.168.20.0:22  PasswordAuthentication no  REMOTECLI  ssh-keygen  ssh-copy-id skill39@192.168.20.1 |
| --- |

## Настройка Windows

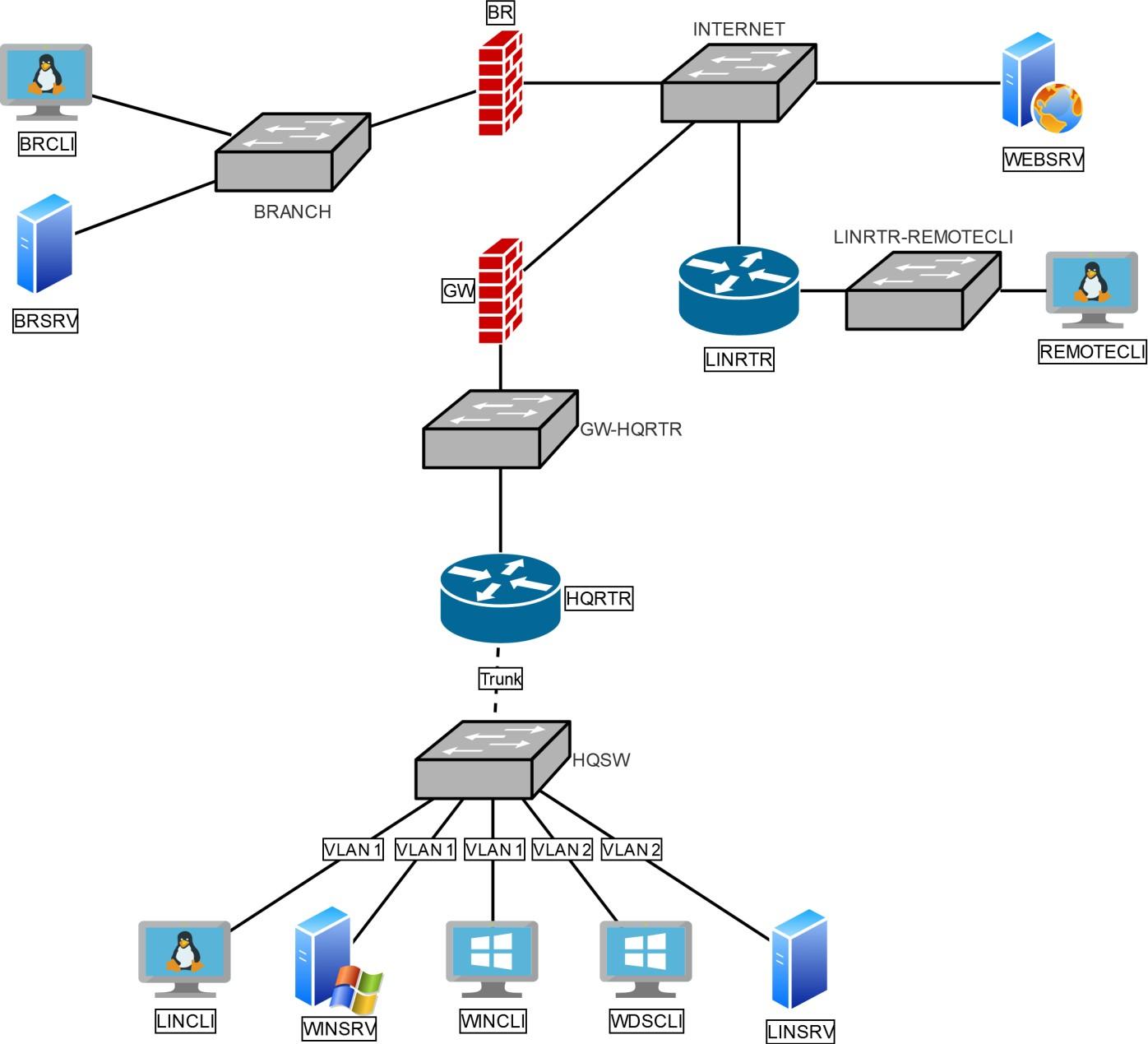
#### Настройка WINSRV

1. Члены группы Engineers должны иметь возможность скачивать и загружать файлы в папку C:\Site по протоколу FTP.

#### Настройка WINCLI

1. Запретите запуск любого исполняемого кода из корневого каталога диска C:. Учтите, что хранение исполняемых файлов в этом каталоге должно оставаться возможным для членов групп локальных и доменных администраторов. Указанный запрет не должен распространяться на WDSCLI.
2. Запросите у ROOTCA сертификат для пользователя Denis и поместите его в хранилище личных сертификатов.

***Топология***

L1-L2

L3